



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/751,596	12/29/2000	Michael N. Gurevich	004537.P004	8571

7590

02/13/2004

Michael J. Mallie
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER

TRUONG, THANHNGA B

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 02/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/751,596

Applicant(s)

GUREVICH ET AL.

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5. 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Ahvenainen (US 6,199, 161).

a. Referring to claim 1:

i. Ahvenainen teaches:

(1) generating a first key component [i.e., the random number RAND being generated in the system (column 1, line 59)];

(2) generating an encryption key using the first key component, a token key and a personal identification number (PIN) [i.e., as shown in Figure 1, a key generator 100, in which the authentication keys, that is “an encryption key”, are generated and programmed in the memories of authentication centers in the system and on the SIM cards (column 8, lines 3-5), wherein the SIM card is “a token key” which include Personal Identification Number (PIN) (column 2, lines 44-45)];

(3) encrypting data using the encryption key [i.e., the encryption keys will not have to be transferred without encryption in the system or with a SIM card (column 7, lines 5-6)];

(4) sending the data encrypted with the encryption key to a server along with the first key component [i.e., referring to Figure 4, the figure shows the network infrastructure (INFRA) 600 of the mobile communication

Art Unit: 2135

system. The network infrastructure comprises e.g. base stations BS (Figure 3), exchanges and other telecommunication devices as well as subscriber databases (that is "a server"), such as a Home Location Register (HLR) and a Visitor Location Register (VLR), and an authentication center (AUC) (column 9, lines 14-21). In addition, the mobile station 500 according to the invention comprises a subscriber equipment which may be provided with a subscriber identity module. The subscriber equipment consists of the transceiver unit 501 (that is for "sending the data encrypted with the encryption key to a server along with the first key component"), the controller 503 and the user interface 505. The mobile station further comprises a unique subscriber identity module 509, e.g. a SIM card, which is detachably connected to the subscriber equipment, thus forming a mobile station (column 10, lines 7-14)].

b. Referring to claim 2:

i. Ahvenainen further teaches:

(1) receiving the token key from a service provider [i.e., if a subscriber identity module e.g. a SIM card, that is "the token key", is employed, the user need not have a mobile equipment of his own, but a subscriber identity module e.g. a SIM card issued to him by the operator of the mobile communication system (column 2, lines 33-36)].

c. Referring to claim 3:

i. Ahvenainen further teaches:

(1) the server storing the first key component and the data encrypted with the encryption key [i.e., in Tetra systems, the authentication key is stored in the mobile communication network in a safe database of a subscriber's home network (column 3, lines 45-47). Furthermore, a method for managing authentication keys in a mobile communication system comprising at least one authentication center, base stations, and mobile stations which are provided with identifiers and which communicate with said base stations and to which subscriber identity modules may be connected, as well as at least one subscriber database which stores each subscriber's subscriber data (column 5,

lines 26-34), in which “first key component and the data encrypted with the encryption key” is considered to include in the subscriber database].

d. Referring to claim 4:

i. Ahvenainen further teaches:

(1) wherein the token key is unique for each user [i.e., the mobile station further comprises a unique subscriber identity module 509, e.g. a SIM card, that is “the token key” (column 10, lines 11-12)].

e. Referring to claim 5:

i. Ahvenainen further teaches:

(1) wherein the first keycomponent is unique for each data entry stored by the server [i.e., The mobile station transmits an enquiry comprising a RAND and a pointer to the network. By means of the pointer, the system finds the correct key K, and by using the RAND computes a result which has to be the same as the one computed in the mobile station (column 8, lines 35-40), that means “the first key component is unique for each data entry stored by the server”].

f. Referring to claim 6:

i. Ahvenainen teaches:

(1) encrypting data using the encryption key generating using a first key component, a token key and a personal identification number (PIN) [i.e., as shown in Figure 1, a key generator 100, in which the authentication keys, that is “an encryption key”, are generated and programmed in the memories of authentication centers in the system and on the SIM cards (column 8, lines 3-5), wherein the SIM card is “a token key” which include Personal Identification Number (PIN) (column 2, lines 44-45). Nevertheless, the encryption keys will not have to be transferred without encryption in the system or with a SIM card (column 7, lines 5-6)];

(2) storing data encrypted using the encryption key [i.e., referring to Figure 1, master authentication center generates the authentication key, which is used for “storing data encrypted”]; and

(3) regenerating the encryption key after accessing the encrypted data to decrypt the encrypted data therewith [i.e., referring again to Figure 1, “regenerating the encryption key after accessing the encrypted data to decrypt the encrypted data therewith” is considered to include in the key generator 100].

g. Referring to claim 7:

i. Ahvenainen further teaches:

(1) disabling the token [i.e., a SIM card blocked, that is “disabling”, by too many attempts of inputting a wrong PIN (column 2, lines 47-48)].

h. Referring to claim 8:

i. Ahvenainen further teaches:

(1) wherein the token is disabled if lost [i.e., a subscriber identity module such as a SIM card does not constitute a threat to security as the divulging does not benefit an unauthorized user in any way in his unauthorized attempts to be authenticated and registered into the mobile communication system (column 7, lines 21-26). In other words, a SIM card blocked, that is “disabling”, by too many attempts of inputting a wrong PIN (column 2, lines 47-48)].

i. Referring to claim 9:

i. This claim has limitations that is similar to those of claims 7 and 8, thus it is rejected with the same rationale applied against claims 7 and 8 above.

j. Referring to claim 10:

i. Ahvenainen further teaches:

(1) re-enabling the token [i.e., a SIM card blocked, that is “disabling”, by too many attempts of inputting a wrong PIN (column 2, lines 47-48), and wherein “re-enabling” the SIM card is inherently provided].

k. Referring to claim 11:

i. Ahvenainen further teaches:

(1) wherein the token ID comprises an alpha-numeric string [i.e., referring to Figure 2, “the token ID comprises an alpha-numeric string” is considered to include in SIM 101, for example subscriber: Patrol 12].

l. Referring to claim 12:

i. Ahvenainen further teaches:

(1) wherein the token key comprises a randomly generated number [i.e., referring to Figure 2, the system employs an index or pointer for pointing to authentication keys in the system. The index, that is “a randomly generated number”, may be located in the subscriber identity module, e.g. in a SIM card 101].

m. Referring to claim 13:

i. Ahvenainen further teaches:

(1) wherein either or both of the token key and PIN comprises biometric data [i.e., referring to Figure 2, “biometric data” is considered to include in the identifier 202 supplied with the card, that is “token key and PIN”].

n. Referring to claim 14:

i. Ahvenainen further teaches:

(1) wherein the token key is the same for all tokens used by the user [i.e., referring to Figure 2, the subscriber receives a SIM card, 101, and his subscriber data are defined in the system, for example in a subscriber database 201 of the system. The authentication key index i.e. the identifier 202 supplied with the card is defined in the subscriber data (column 8, lines 44-48)].

o. Referring to claim 15:

i. Ahvenainen further teaches:

(1) monitoring browsing activities; identifying web pages containing a form; and inserting content into the form [i.e., referring to Figure 4, “monitoring browsing activities; identifying web pages containing a form; and inserting content into the form” are considered to include in the mobile station 500].

p. Referring to claims 16, 17, 18, and 19:

i. These claims have limitations that is similar to those of claim 15, thus they are rejected with the same rationale applied against claim 15 above.

q. Referring to claim 20:

i. Ahvenainen teaches:

(1) retrieving a key component and encrypted data from a server [i.e., referring to Figure 1, when registering a mobile station or its user, an identifier stored in a subscriber identity module SIM, 101 according to the invention is transmitted from the mobile station being discussed to a base station BS of the mobile communication system. Following this, on the basis of said identifier, an authentication key corresponding to said identifier 202 will be searched from an authentication center AUC,102. On the basis of the identifier 202, the authentication desired is carried out by means of the authentication key retrieved (column 8, lines 16-25). In addition, the mobile communication system may additionally have another authentication center in reserve, i.e. a backup authentication center 103, that is for “retrieving a key component and encrypted data from a server” (column 8, lines 12-14)];

(2) recreating an encryption key using the key component, a token key and a personal identification number (PIN) [i.e., as shown in Figure 1, a key generator 100, that is for “recreating an encryption key using the key component, a token key and a personal identification number (PIN)”]; and

(3) performing a decryption operation on the encrypted data using a decryption key based on the encryption key used to encrypt the encrypted [i.e., referring to Figure 1, it shows a master authentication center 102, that is for “performing a decryption operation on the encrypted data using a decryption key based on the encryption key used to encrypt the encrypted”, in which the actual authentication takes place (column 8, lines 10-11)].

r. Referring to claim 21:

i. Ahvenainen teaches:

(1) generating authentication data for a user based on a token key and a personal identification number (PIN), the token key being unique to the

user [i.e., referring to Figure 1, it shows a master authentication center 102, that is for “generating authentication data for a user based on a token key and a personal identification number (PIN)”, in which the actual authentication takes place (column 8, lines 10-11). In addition, the mobile station further comprises a unique subscriber identity module 509, e.g. a SIM card, that is “the token key” (column 10, lines 11-12)]; and

(2) receiving a confirmation indicating that the authentication data has been verified [i.e., when registering a mobile station or its user, an identifier in accordance with the invention, which is stored in a subscriber database DB, is transmitted during the authentication process to the authentication center 102, AUC. Following this, the authentication is carried out by means of the authentication key retrieved on the basis of said identifier. It should be noted that by means of said authentication key it is possible to authenticate either a mobile station or its user, or the mobile communication system (column 8, lines 25-35), whereby the authentication center 102, that is for “receiving a confirmation indicating that the authentication data has been verified”].

s. Referring to claim 22:

i. Ahvenainen teaches:

(1) accessing encrypted data from a server [i.e., when registering a mobile station or its user, an identifier stored in a subscriber identity module SIM, 101 according to the invention is transmitted from the mobile station being discussed to a base station BS of the mobile communication system. Following this, on the basis of said identifier, an authentication key corresponding to said identifier 202 will be searched, that is “accessed”, from an authentication center AUC 102. On the basis of the identifier 202, the authentication desired is carried out by means of the authentication key retrieved (column 8, lines 16-25)];

(2) decrypting the encrypted data using a token and a user-specific PIN to be accessed [i.e., referring to Figure 1, it shows a master

authentication center 102, that is for “decrypting the encrypted data using a token and a user-specific PIN to be accessed”, in which the actual authentication takes place (column 8, lines 10-11)].

t. Referring to claim 23:

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

u. Referring to claim 24:

i. Ahvenainen further teaches:

(1) wherein the token comprises a utility to manage data depending on data type [i.e., **the functions, that is “a utility to manage data depending on data type”, of the SIM card on the one hand include providing the mobile station with data indicating the user in a well protected manner and on the other hand to offer services to the mobile station. Such services may include e.g. maintaining (inputting, changing) a Personal Identification Number (PIN), maintaining the data protection key i.e. the authentication key K, and unblocking by e.g. a PUK code, Personal Unblocking Key, a SIM card blocked by too many attempts of inputting a wrong PIN (column 2, lines 40-48)].**

v. Referring to claims 25 and 66:

i. These claims have limitations that is similar to those of claims 15 and 24, thus they are rejected with the same rationale applied against claims 15 and 24 above.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kelly (US 6, 044, 154) discloses a security system is disclosed, which system is for granting access to a host computer in response to a demand from a remote computer. The security system has a permanent encryption key mounted on the remote computer (see abstract).

b. Audebert (US 5, 937, 068) discloses the system includes a first card-like unit adapted to communicate with a second unit giving only conditionally

Art Unit: 2135

access to a function. Both units are capable of running software for generating a password by means of encryption of a plurality of dynamic variables produced separately but in concert (so as to have a predetermined relationship, such as identity, with one another) in the units (see abstract).


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

February 4, 20044



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100